NON-ABELIAN LITTLEWOOD-OFFORD INEQUALITIES

PHAM H. TIEP AND VAN H. VU

Abstract. In 1943, Littlewood and Offord proved the first anti-concentration result for sums of independent random variables. Their result has since then been strengthened and generalized by generations of researchers, with applications in several areas of mathematics.

In this paper, we present the first non-abelian analogue of Littlewood-Offord result, a sharp anti-concentration inequality for products of independent random variables.

1. Introduction

In 1943, motivated by their studies of random polynomials, Littlewood and Offord [LO] proved a remarkable fact about the distribution of a sum of independent random variables. Let V be a sequence of (not necessarily different) non-zero real numbers $a_1, \dots, a_n$ and set

$$\rho_V := \sup_{b \in \mathbb{R}} \mathbf{P}(\sum_{i=1}^{n} \hat{a}_i = b),$$

where the $\hat{a_i}$ are independent random variables taking values $\pm a_i$ with probability $1/2$.

Theorem 1.1.

$$\rho_V = O(n^{-1/2} \log n).$$

Here and hereafter, the asymptotic notation is used under the assumption that $n \to \infty$. Soon after their paper, Erdős [E], removing the $\log n$ term, optimized the bound.

Theorem 1.2. *(Littlewood-Offord-Erdős)*

$$\rho_V \leq \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O(n^{-1/2}).$$

The bound is sharp, as shown by taking all $a_i = 1$. It is easy to see that in this case $\mathbf{P}(\sum_{i=1}^{n} \hat{a}_i = \delta) = \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n}$, where $\delta = 1$ if n is odd and 0 otherwise. In [Kle1], Kleitman generalized Theorem 1.2 to complex setting.

It is best to relate Theorem 1.2 to the classical Berry-Esseen theorem, which asserts that if the a_i are all of magnitude 1, then the distribution of $\frac{1}{\sqrt{n}} \sum_i^n \hat{a}_i$ converges to the normal distribution with rate $O(n^{-1/2})$. This implies that for any point b, $\mathbf{P}(\sum_{i=1}^{n} \hat{a}_i = b) = O(n^{-1/2})$. Theorem 1.2 strengthens this fact significantly, asserting that the probability in question is always $O(n^{-1/2})$, *regardless of the magnitude of the* a_i.

2010 *Mathematics Subject Classification.* 05D40, 20C33 (Primary), 60B15, 60C05, 60G50 (Secondary).

Key words and phrases. Littlewood-Offord-Erdős theorem, anti-concentration inequalities.

P. H. Tiep gratefully acknowledges the support of the NSF (grant DMS-1201374) and the Simons Foundation Fellowship 305247.

V. H. Vu is supported by research grants DMS-0901216 and AFOSAR-FA-9550-09-1-0167.

Theorem 1.2 has become the starting point of a long line of research, which continues through several decades and has recently becomes very active (see, for instance, the survey [NV]). It has been strengthened (under various conditions) and generalized in different directions by many researchers, including Esseen, Kolmogorov, Rogozin, Halász, Stanley, Kleitman, Szemerédi-Sárközy, Tao, and others; see, for instance [EM, Es, FF, Gr, H, Kle1, Kle2, Kle3, Ng, Ngv, Rog, SSz, RV, TV1, TV2, TV3, St]. These results are often referred to as anti-concentration inequalities, and have found surprising applications in different areas of mathematics, including random matrix theory. For more details, the reader may want to check the recent survey [NV].

A limitation to all existing extensions of Theorem 1.2 is that they only apply for random variables taking values in an abelian group (in most cases $\mathbb{R}^d$ or $\mathbb{C}$), as the available proof techniques only work in this setting.

The goal of this paper is to initiate the study of the anti-concentration phenomenon in the non-abelian setting. Let V be a sequence of (not necessarily distinct) non-trivial elements $A_1, \dots, A_n$ of a non-abelian group G and set

$$\rho_V := \sup_{B \in G} \mathbf{P}(\prod_{i=1}^{n} \hat{A}_i = B),$$

where the $\hat{A}_i$ are independent random variables taking values A_i or A_i^{-1} with probability $1/2$.

In what follows, we work toward the most natural non-abelian extension of Theorem 1.2 with the A_i being invertible matrices of a fixed size m. Our goal is to bound ρ_V. Thanks to the famous work of Furstenberg and Kesten [FK], a central limit theorem for products of i.i.d. random matrices is known, and Berry-Essen type local central limit theorems are also available; see for instance [LV] and the references therein. But in the cases where central limit theorems fail, our result provides the first anti-concentration inequality.

In view of Theorem 1.2, it is tempting to guess that $\rho_V = O(n^{-1/2})$. There are several constructions matching this bound.

Example 1. Let A be an invertible $m \times m$ matrix over some field $\mathbb{F}$ of infinite order (as an element of $GL_m(\mathbb{F})$), and $A_i = A$ all $1 \le i \le n$. Then

$$\mathbf{P}(\prod_{i=1}^{n} \hat{A}_i = \Delta) = \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = \Theta(n^{-1/2})$$

where $\Delta = A$ if n is odd and I (the identity matrix) if n is even.

Example 2. Let

$$A_i = \begin{bmatrix} 1 & a_i \\ 0 & 1 \end{bmatrix}$$

where a_i is an integer with absolute value at most K, where $1 \le K = O(1)$. We have

$$A_i A_j = \begin{bmatrix} 1 & a_i + a_j \\ 0 & 1 \end{bmatrix}, \ A_i^{-1} = \begin{bmatrix} 1 & -a_i \\ 0 & 1 \end{bmatrix}.$$

The top right corner of the random product $\prod_{i=1}^n \hat{A}_i$ is the random sum $S := \sum_{i=1}^n \hat{a}_i$, which has mean 0 and variance $\sum_{i=1}^n a_i^2 \leq nK^2$. By Chebyshev's inequality, with probability at least 3/4, $|S| \leq 2Kn^{1/2}$. By the pigeonhole principle, there is an integer s such that

$$\mathbf{P}(S = s) \geq \frac{3}{4} \cdot \frac{1}{2Kn^{1/2} + 1} \geq \frac{1}{4Kn^{1/2}}.$$

It follows that

$$\rho_V \geq \frac{1}{4K} n^{-1/2}.$$

However, the presence of torsions makes the problem more subtle than its abelian counterparts. Assume that all $A_i = A$ and A has order s, then the product $\prod_{i=1}^n \hat{A}_i$ can take only s values $A, A^2, \ldots, A^{s-1}, A^s = I$ (where I again denotes the identity matrix). By the pigeonhole principle, it follows that

$$\rho_V \geq \frac{1}{s}.$$

We are now ready to state our main results, which are sharp with respect to the above examples.

Theorem 1.3. *For any integers $m, n, s \geq 2$ the following statement holds. Let V be a sequence $A_1, \ldots, A_n$ of elements of $GL_m(\mathbb{C})$ of order at least s. Then*

$$\rho_V \leq 141 \cdot \max\left\{\frac{1}{s}, \frac{1}{\sqrt{n}}\right\}.$$

Our approach also yields the following theorem.

Theorem 1.4. *Let $m, n, s \geq 2$ be integers and let $p \geq \min\{s, \sqrt{n}\}$ be a sufficiently large prime. Let V be a sequence $A_1, \ldots, A_n$ of elements of $GL_m(p)$ of order at least s. Then*

$$\rho_V \leq 141 \cdot \max\left\{\frac{1}{s}, \frac{1}{\sqrt{n}}\right\}.$$

We can generalize Theorem 1.3 to the following

Theorem 1.5. *For any integers $m, n, s \geq 2$ the following statement holds. Let V be a sequence $A_1, \ldots, A_n$ of elements of $GL_m(\mathbb{C})$ where at least N of them have order at least s. Then*

$$\rho_V \leq 141 \cdot \max\left\{\frac{1}{s}, \frac{1}{\sqrt{N}}\right\}.$$

Remark 1.6. The above theorems also hold for all groups which can be embedded into $GL_m(p)$ or $GL_m(\mathbb{C})$. The word *embed* can be interpreted in two ways. First, one can use canonical embeddings, such as embeddings of simple Lie groups into $GL_m(\mathbb{C})$, or more generally, embeddings via faithful finite-dimensional complex representations. In particular, Theorem 1.5 holds for any arbitrary group G that admits a faithful finite-dimensional complex representation. Next, one can also use the embeddings discussed in Section 2. The reader is invited to work out an example. The term 141 can be improved somewhat, but we do not try to push in this direction.

Our proof combines tools from three different areas: additive combinatorics, representation theory and linear algebra, and we also use results from analytic number theory. First, Section 2 provides us with Freiman-like embeddings that allow us to map our problems from infinite settings to a finite setting of $GL_m(p)$, with the prime p chosen suitably. Next, in Section 3 we prove the key Proposition 3.3 which shows that, if m or p is sufficiently large and Φ is an irreducible complex representation of $SL_m(q)$ (with $p|q$), then the eigenvalues of $\Phi(g)$ for any non-central element $g \in SL_m(q)$ have an "almost" uniform distribution. In Sections 4 and 5, we give a representation-theoretic formula for the probability in question, and provide a way to bound it from the above by using estimates on singular values. The proofs of the main results will then be presented in Section 6.

Notation. The asymptotic notation is used under the assumption that $n \to \infty$. For a group G, $\mathbf{Z}(G)$ is its center, $\mathrm{Irr}(G)$ denotes the set of isomorphism classes of its irreducible representations (or the set of its complex irreducible characters, depending on the context), $\langle X \rangle$ denotes the subgroup generated by a subset X of G, $\mathbf{1}$ denotes the identity element. In the matrix setting, I denotes the identity matrix. For an element $g \in G$, we denote by $\mathbf{o}(g)$ its order, and $\mathbf{C}_G(g)$ its centralizer. If α and β are complex characters of a finite group G, then $[\alpha, \beta]_G$ denotes their scalar product, and α_H denotes the restriction of α to a subgroup $H \leq G$. $\mathbf{P}, \mathbf{E}, \mathbf{I}_E$ denote probability, expectation, indicator variable of an event E, respectively.

2. Embedding theorems

In this section, we discuss results that allow us to map our problem from an infinite setting (the underlying group is infinite) to a finite setting (the underlying group is finite) and vice versa. Let us start with the following result, which is a special case of [VWW, Theorem 1.1].

Theorem 2.1. *Let S be a finite collection of complex numbers and L a finite collection of non-zero elements of $\mathbb{Z}[S]$. Then there is an infinite sequence $\mathcal{P}$ of primes p such that for any $p \in \mathcal{P}$, there is a ring homomorphism Φ from $\mathbb{Z}[S]$ to $\mathbb{Z}/p\mathbb{Z}$ such that $0 \notin \Phi(L)$.*

We obtain the following corollary.

Corollary 2.2. *Let $A_1, \dots, A_n$ be (not necessarily distinct) elements of $GL_m(\mathbb{C})$. Then there is an infinite sequence $\mathcal{P}$ of primes p such that for any $p \in \mathcal{P}$, there is a group homomorphism Φ from $\langle A_1, \dots, A_n \rangle$ to $GL_m(p)$ such that*

(i) *If $\mathbf{o}(A_i) < \infty$, then $\mathbf{o}(\Phi(A_i)) = \mathbf{o}(A_i)$;*
(ii) *If $\mathbf{o}(A_i) = \infty$, then $\mathbf{o}(\Phi(A_i)) \geq n$.*

Proof. Let $S \subset \mathbb{C}$ be the set consisting of all the entries of the A_i and their complex conjugates. For each i, let $d_i = \min\{n, \mathbf{o}(A_i)\}$. For each $1 \leq j \leq d_i - 1$, $1 \leq k, l \leq m$, let $F_{i,j,k,l}$ be the (k,l)-th entry of A_i^j. It is clear that both $F_{i,j,k,l}$ and $\bar{F}_{i,j,k,l}$ are polynomials in S with integer coefficients. Define

$$G(i,j) := \sum_{1 \leq k \neq l \leq m} F_{i,j,k,l}\bar{F}_{i,j,k,l} + \sum_{k=1}^{m} (F_{i,j,k,k} - 1)(\bar{F}_{i,j,k,k} - 1).$$

Again $G(i,j)$ is a polynomial in S with integer coefficients. More importantly, $G(i,j) = 0$ iff $A_i^j = I$. Now we apply Theorem 2.1 with L being the collection of the $G(i,j)$ for all

possible pairs i, j. The map from $\langle A_1, \dots, A_n \rangle$ to $GL_m(p)$ is induced trivially by the map from $\mathbb{Z}[S]$ to $\mathbb{Z}/p\mathbb{Z}$. □

3. Representation theory

Our study will make use of several non-trivial facts about the irreducible representations of a finite group, the most critical one being an estimate on the multiplicities of the eigenvalues. Let us start with a toy lemma.

Lemma 3.1. *Let G be a finite group and let Φ be a complex irreducible representation of G with character χ. Suppose there is a constant $0 < \alpha < 1$ such that $|\chi(x)/\chi(1)| \leq \alpha$ for all $x \in G \setminus \mathbf{Z}(G)$. If $g \in G \setminus \mathbf{Z}(G)$ is such that $g\mathbf{Z}(G)$ has order k_1 in $G/\mathbf{Z}(G)$, then the multiplicity m of any eigenvalue of $\Phi(g)$ satisfies*

$$(k_1^{-1} - \alpha)(\dim \Phi) < m < (k_1^{-1} + \alpha)(\dim \Phi).$$

Proof. Let k be the order of g in G and let $\varepsilon \in \mathbb{C}$ be a primitive k-th root of unity. Then $k_1 \mid k$ and $g^{k_1} \in \mathbf{Z}(G)$. By Schur's Lemma, $\Phi(g^{k_1}) = \varepsilon^{k_1 l} I$ for some $l \in \mathbb{N}$. It follows that if λ is any irreducible constituent of the character χ of Φ restricted to $C := \langle g \rangle$, then $\lambda(g^{k_1}) = \varepsilon^{k_1 l}$ and $\chi(g^i) = \chi(1)\lambda(g^i)$ if $k_1 | i$. By assumption, $|\chi(g^i)| \leq \alpha\chi(1)$ if $k_1 \nmid i$. Now,

$$[\chi_C, \lambda]_C = \left| \frac{1}{k} \sum_{i=0}^{k-1} \chi(g^i)\bar{\lambda}(g^i) \right| \leq \frac{1}{k} \left(\left| \sum_{k_1 | i} \chi(g^i)\bar{\lambda}(g^i) \right| + \sum_{k_1 \nmid i} |\chi(g^i)\bar{\lambda}(g^i)| \right)$$

$$\leq \frac{\chi(1)}{k} \left(\frac{k}{k_1} + \alpha(k - k_1) \right) < \chi(1)(k_1^{-1} + \alpha).$$

The lower bound $[\chi_C, \lambda]_C > \chi(1)(k_1^{-1} - \alpha)$ is proved similarly. □

Corollary 3.2. *Let $G = SL_d(q)$ with $d \geq 2$ and $q \geq 49$. Suppose that Φ is a complex irreducible representation of degree > 1 of G and $g \in G \setminus \mathbf{Z}(G)$ is such that $g\mathbf{Z}(G)$ has order k_1 in $G/\mathbf{Z}(G)$. Then the multiplicity m of any eigenvalue of $\Phi(g)$ satisfies*

$$(k_1^{-1} - \alpha)(\dim \Phi) < m < (k_1^{-1} + \alpha)(\dim \Phi)$$

with $\alpha := 1/(\sqrt{q} - 1)$.

Proof. By Theorems 3.3 and 5.3 of [G], G satisfies the hypothesis of Lemma 3.1 with the specified α. Hence the statement follows. □

Notice that if $g\mathbf{Z}(G)$ has order k_1 in $G/\mathbf{Z}(G)$, then its eigenvalues are among the k_1-th roots of unity of a fixed complex number. Corollary 3.2 asserts that each eigenvalue appears about $(\dim \Phi)/k_1$ times. However, this result is not sufficiently strong for our purposes if the term α dominates. In applications, we will need the following more precise statement which we formulate for both $G = SL_d(q)$ and $S = PSL_(q) = G/\mathbf{Z}(G)$.

Proposition 3.3. *Let $H \in \{G, S\}$ where $G = SL_d(q)$ and $S = PSL_d(q)$ with $d \geq 3$ and $q \geq 11$. Set $e := \gcd(d, q-1)$ and $e_H := |\mathbf{Z}(H)|$ so that $e_G = e$ and $e_S = 1$.*

(i) *$|\operatorname{Irr}(G)| \leq q^{d-1} + 3q^{d-2} \leq (14/11)q^{d-1}$ and $|\operatorname{Irr}(S)| \leq (q^{d-1} + 5q^{d-2})/e \leq (16/11e)q^{d-1}$. Furthermore,*

$$\sum_{\chi \in \operatorname{Irr}(H),\ \chi(1) < q^{(d^2-d-1)/2}} \chi(1)^2 < \frac{5}{3q} \cdot |H|.$$

(ii) *Suppose that* $\chi \in \mathrm{Irr}(H)$ *satisfies* $\chi(1) \geq q^{(d^2-d-1)/2}$ *and* $x \in H \setminus \mathbf{Z}(H)$. *Then*

$$\frac{|\chi(x)|}{\chi(1)} \leq q^{(3-d)/2}.$$

(iii) *Suppose that* $q = p^f$ *is a power of a prime* $p \geq d$. *Then for any* $x \in H$, *we have that* $\mathbf{o}(x) < q^{d+1}$; *furthermore, either* $|\mathbf{C}_H(x)| \leq q^{d^2-4d+8}$ *or* $\mathbf{o}(x) < q^2$.

(iv) *Suppose that* $d \geq 43$, $q = p \geq d$, *and* p *or* d *is chosen sufficiently large. For any element* $g \in H \setminus \{1\}$ *of order say* N, *if* Φ *is a complex irreducible representation of* H *of degree* $\geq q^{(d^2-d-1)/2}$, *then any eigenvalue of* $\Phi(g)$ *occurs with multiplicity at most* $(e_H + 2)(\dim \Phi)/N$.

Proof. (i) The first two inequalities are just Proposition 3.6(2) and Corollary 3.7(2) of [FG]. Next, by [LMT, Lemma 4.1(i)] we have

$$\frac{|G|}{q^{d^2-1}} > \prod_{i=1}^{\infty}(1 - q^{-i}) > 1 - \frac{1}{q} - \frac{1}{q^2} \geq \frac{109}{121}$$

as we assume $q \geq 11$. It follows that

$$\frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) < q^{(d^2-d-1)/2}} \chi(1)^2 < \frac{|\mathrm{Irr}(G)| \cdot q^{d^2-d-1}}{|G|} < \frac{(14/11) \cdot q^{d^2-2}}{(109/121) \cdot q^{d^2-1}} < \frac{3}{2q}.$$

Next, as $|S| = |G|/e$, we have

$$\frac{1}{|S|} \sum_{\chi \in \mathrm{Irr}(S),\ \chi(1) < q^{(d^2-d-1)/2}} \chi(1)^2 < \frac{|\mathrm{Irr}(S)| \cdot q^{d^2-d-1}}{|S|} < \frac{(16/11e) \cdot q^{d^2-2}}{(109/121e) \cdot q^{d^2-1}} < \frac{5}{3q}.$$

(ii) As mentioned in the proof of [LST, Proposition 6.2.1], $|\mathbf{C}_G(x)| \leq q^{d^2-2d+2}$. As $|\chi(x)| \leq |\mathbf{C}_G(x)|^{1/2}$, the claim follows for $H = G$. The claim for $H = S$ follows in a similar fashion, by noting that

$$|\mathbf{C}_S(x)| \leq |\mathbf{C}_G(\hat{x})| \tag{3.1}$$

if $x \in S = G/\mathbf{Z}(G)$ and $\hat{x}$ is an inverse image of x in G. (Indeed, let D be the complete inverse image of $\mathbf{C}_S(x)$ in G. Then, for any $g \in D$ we have $g\hat{x}g^{-1} = \hat{x}f(g)$ for some element $f(g) \in \mathbf{Z}(G)$. It is easy to see that $f \in \mathrm{Hom}(D, \mathbf{Z}(G))$ with $\mathrm{Ker}(D) = \mathbf{C}_G(\hat{x})$. Hence, $|D| \leq |\mathbf{Z}(G)| \cdot |\mathbf{C}_G(\hat{x})|$, and so

$$|\mathbf{C}_S(x)| = |D/\mathbf{Z}(G)| \leq |\mathbf{C}_G(\hat{x})|.)$$

(iii) First we prove the claims for $H = G$. Write $x = su$ as a commuting product of a semisimple element $s \in G$ and a unipotent element $u \in G$; in particular, $\mathbf{o}(x) = \mathbf{o}(s) \cdot \mathbf{o}(u)$. The condition $p \geq d$ implies that

$$\mathbf{o}(u) \leq p \leq q.$$

Next, we consider the characteristic polynomial $f(t) \in \mathbb{F}_q[t]$ of the semisimple linear transformation s of the vector space $V = \mathbb{F}_q^d$. We also decompose $f(t) = \prod_{i=1}^m f_i(t)^{k_i}$ as a product of powers of pairwise distinct monic irreducible polynomials $f_i \in \mathbb{F}_q[t]$, with $\deg f_i = a_i$, so

that $\sum_{i=1}^m k_i a_i = d$. Then both s and $\mathbf{C}_G(s)$ preserve a direct sum decomposition $V = \oplus_{i=1}^m V_i$ where $\dim V_i = k_i a_i$, and the action of s on V_i has order at most $q^{a_i} - 1$. It follows that

$$\mathbf{o}(s) \leq \prod_{i=1}^m (q^{a_i} - 1) \leq q^{\sum_{i=1}^m a_i} - 1 \leq q^d - 1,$$

implying $\mathbf{o}(x) = \mathbf{o}(s) \cdot \mathbf{o}(u) < q^{d+1}$ as stated. We also note that

$$\mathbf{C}_G(s) \hookrightarrow GL_{k_1}(q^{a_1}) \times GL_{k_2}(q^{a_2}) \times \ldots \times GL_{k_m}(q^{a_m}). \tag{3.2}$$

Suppose in addition that $|\mathbf{C}_G(x)| > q^{d^2-4d+8}$. As the semisimple part s of x is a power of x, we also have that $|\mathbf{C}_G(s)| > q^{d^2-4d+8}$. It suffices to show that in this case $\mathbf{o}(s) \leq q - 1$. We may assume that

$$k_1 a_1 \geq k_2 a_2 \geq \ldots \geq k_m a_m. \tag{3.3}$$

If $m = 1$ and $a_1 \geq 2$, then (3.2) implies that

$$|\mathbf{C}_G(s)| \leq |GL_{k_1}(q^{a_1})| < q^{k_1^2 a_1} = q^{d^2/a_1} \leq q^{d^2/2} \leq q^{(d^2-4d+8)},$$

contrary to the assumption. On the other hand, if $a_1 = 1$, then $k_1 = d$ and so $s \in \mathbf{Z}(G)$ and $\mathbf{o}(s) \leq q - 1$ as desired. So we may assume that $m \geq 2$. Suppose now that $k_1 a_1 =: k \geq 2$ and $d - k \geq 2$. Then, as $\mathbf{C}_G(s)$ preserves the decomposition $V = \oplus_{i=1}^m V_i$, we have that

$$|\mathbf{C}_G(s)| \leq |GL(V_1) \times GL(\oplus_{i=2}^m V_i)| = |GL_k(q) \times GL_{d-k}(q)| < q^{k^2+(d-k)^2} \leq q^{d^2-4d+8},$$

again a contradiction. If $k = 1$, then the choice (3.3) implies that $k_i a_i = 1$ for all i and so $\mathbf{C}_G(s) \leq GL_1(q)^d$ by (3.2), whence $\mathbf{o}(s) \leq q-1$. So we may assume $k = d-1$. If furthermore $a_1 \geq 2$, then again by (3.2) we have

$$|\mathbf{C}_G(s)| \leq |GL_{k_1}(q^{a_1}) \times GL_1(q)| < q^{k_1^2 a_1 + 1} = q^{(d-1)^2/a_1 + 1} \leq q^{(d^2-2d+3)/2} < q^{d^2-4d+8},$$

contrary to the assumption. Thus $(m, k_1, a_1, k_2, a_2) = (2, d-1, 1, 1, 1)$, in which case we again have $\mathbf{o}(s) \leq q - 1$.

Now we prove the claims for $H = S$. Let $x \in S = G/\mathbf{Z}(G)$ and let $\hat{x}$ be an inverse image of x in G. Then it is clear that

$$\mathbf{o}(x) \leq \mathbf{o}(\hat{x}). \tag{3.4}$$

As $\mathbf{o}(\hat{x}) \leq q^{d+1}$, we also have $\mathbf{o}(x) \leq q^{d+1}$. Next, we have shown that either $|\mathbf{C}_G(\hat{x})| \leq q^{d^2-4d+8}$, in which case $|\mathbf{C}_S(x)| \leq q^{d^2-4d+8}|$ by (3.1), or $\mathbf{o}(\hat{x}) \leq q^2$, in which case $\mathbf{o}(x) \leq q^2$ by (3.4).

(iv) Let M denote the largest multiplicity of any eigenvalue of $\Phi(g)$ and let N_1 denote the order of $x\mathbf{Z}(H)$ in $H/\mathbf{Z}(H)$. Then $x^{N_1} \in \mathbf{Z}(H)$ and so $x^{N_1 e_H} = 1$. It follows that $N | N_1 e_H$; in particular, $N_1 \geq N/e_H$. Now, if $N \leq q^{(d-3)/2}$, then (ii) and the proof of Lemma 3.1 (with $\alpha := q^{(3-d)/2}$) show that

$$M \leq (\dim \Phi)(q^{(3-d)/2} + 1/N_1) \leq (\dim \Phi)(q^{(3-d)/2} + e_H/N) \leq (e_H + 1)(\dim \Phi)/N.$$

Now we may assume that $N > q^{(d-3)/2}$. Consider and any element $g^i \notin \mathbf{Z}(H)$. Note by (iii) that $N < q^{d+1}$. If $|g^i| \geq q^2$, then by (iii) we have that

$$|\chi(g^i)| \leq |\mathbf{C}_H(g^i)|^{1/2} \leq q^{(d^2-4d+8)/2} < (\dim \Phi)/q^{d+1} < (\dim \Phi)/N. \tag{3.5}$$

On the other hand, if $|g^i| < q^2$, then, as $d \geq 43$, $|g^i| \leq N^{0.1}$. The number L of such elements g^i is at most the sum of all divisors of N that do not exceed $N^{0.1}$. If p or d is chosen

sufficiently large, then $N > p^{(d-3)/2}$ is large enough, so that the total number of divisors of N is at most $N^{0.2}$, cf. [Ap, p. 296]. It follows that

$$L \le N^{0.1} \cdot N^{0.2} = N^{0.3}. \tag{3.6}$$

Certainly, as $g^i \notin \mathbf{Z}(H)$ and $N < q^{d+1}$ we have by (ii) that

$$|\chi(g^i)|/\chi(1) \le q^{(3-d)/2} < N^{-1/3}. \tag{3.7}$$

Now we can follow the proof of Lemma 3.1 and obtain by (3.5)–(3.7) that the multiplicity of any irreducible constituent λ of χ_C is

$$[\chi_C, \lambda]_C = \left| \frac{1}{N} \sum_{i=0}^{N-1} \chi(g^i)\bar{\lambda}(g^i) \right|$$

$$\le \frac{1}{N} \left(\sum_{g^i \in \mathbf{Z}(H)} |\chi(g^i)\bar{\lambda}(g^i)| + \sum_{g^i \notin \mathbf{Z}(H),\ |g^i| < q^2} |\chi(g^i)\bar{\lambda}(g^i)| + \sum_{|g^i| \ge q^2} |\chi(g^i)\bar{\lambda}(g^i)| \right)$$

$$\le \frac{\chi(1)}{N} \left(e_H + \frac{L - e_H}{N^{1/3}} + \frac{N - L}{N} \right) < \frac{(e_H + 2)\chi(1)}{N},$$

if χ is the character of Φ and $C = \langle g \rangle$. It follows that $M \le (e_H + 2)(\dim \Phi)/N$. □

4. A trace identity

Let G be a finite group. Let $A_1, \dots, A_n, B$ be (not necessarily distinct) elements of G. As usual, $\hat{A}_i$ denotes the random variable taking values A_i and A_i^{-1} with probability $1/2$. The following identity plays an important role in our proof.

Lemma 4.1.

$$\mathbf{P}(\prod_{i=1}^{n} \hat{A}_i = B) = \frac{1}{|G|} \sum_{\Phi \in \mathrm{Irr}(G)} (\dim \Phi) \operatorname{trace} \left(\prod_{i=1}^{n} \frac{\Phi(A_i) + \Phi(A_i^{-1})}{2} \Phi(B^{-1}) \right). \tag{4.1}$$

Proof. Consider the regular representation R of G. It is the direct sum of $\dim(\Phi)$ copies of each $\Phi \in \mathrm{Irr}(G)$ and for any $X \in G$, $\operatorname{trace}(R(X))$ equals $|G|$ if $X = \mathbf{1}$ and 0 otherwise. In other words,

$$\mathbf{I}_{X=\mathbf{1}} = \frac{1}{|G|} \operatorname{trace}(R(X)).$$

Now let $X := \prod_{i=1}^{n} \hat{A}_i B^{-1}$. We have

$$\mathbf{P}(\prod_{i=1}^{n} \hat{A}_i = B) = \mathbf{E} I_{X=\mathbf{1}} = \frac{1}{|G|} \mathbf{E} \operatorname{trace} R(X).$$

By linearity of expectation,

$$\mathbf{E} \operatorname{trace} R(X) = \mathbf{E} \sum_{\Phi \in \mathrm{Irr}(G)} (\dim \Phi) \operatorname{trace} \Phi(X) = \sum_{\Phi \in \mathrm{Irr}(G)} (\dim \Phi) \mathbf{E} \operatorname{trace} \Phi(X).$$

Furthermore, by linearity of trace

$$\mathbf{E}\,\mathrm{trace}\,\Phi(X) = \mathrm{trace}\,\mathbf{E}\Phi(X) = \mathrm{trace}\,\mathbf{E}\prod_{i=1}^{n}\Phi(\hat{A}_i)\Phi(B^{-1}).$$

As the $\hat{A}_i$ are independent,

$$\mathbf{E}\prod_{i=1}^{n}\Phi(\hat{A}_i)\Phi(B^{-1}) = \prod_{i=1}^{n}\mathbf{E}\Phi(\hat{A}_i)\Phi(B^{-1}) = \prod_{i=1}^{n}\frac{\Phi(A_i)+\Phi(A_i^{-1})}{2}\Phi(B^{-1}),$$

concluding the proof. □

5. Singular value estimates

For any complex $n \times n$-matrix M, let $s_1(M) \geq s_2(M) \geq \ldots \geq s_n(M)$ denote the singular values of M (listed in non-increasing order). The evaluation of (4.1) relies on several singular value estimates, which we collect in the following lemma.

Lemma 5.1. *Let M, M' be square matrices of size n. Then*

$$|\,\mathrm{trace}\,M| \leq \sum_{i=1}^{n} s_i(M).$$

Furthermore, for any $1 \leq k \leq n$,

$$s_k(MM') \leq \min\{s_k(M)s_1(M'), s_1(M)s_k(M')\},$$

and

$$\prod_{j=1}^{k} s_j(MM') \leq \prod_{j=1}^{k} s_j(M)\prod_{j=1}^{k} s_j(M').$$

Proof. To prove the first statement, notice that the singular value decomposition yields $M = UDV$, where $U = (u_{ij})$ and $V = (v_{ij})$ are unitary and

$$D = \mathrm{diag}(s_1(M), s_2(M), \ldots, s_n(M)).$$

Next, for a given j,

$$|\sum_{i=1}^{n} u_{ij}v_{ji}| \leq (\sum_{i=1}^{n}|u_{ij}|^2)^{1/2}(\sum_{i=1}^{n}|v_{ji}|^2)^{1/2} = 1.$$

Hence,

$$|\,\mathrm{trace}\,M| = |\sum_{i,j=1}^{n} u_{ij}s_j(M)v_{ji}| \leq \sum_{j=1}^{n} s_j(M)|\sum_{i=1}^{n} u_{ij}v_{ji}| = \sum_{j=1}^{n} s_j(M).$$

The second statement follows from the min-max definition of singular values [Bh, Problems III.6.1, III.6.2].

To prove the third, consider the wedge product $\wedge^k M$. We have by the second statement

$$s_1(\wedge^k(MM')) \leq s_1(\wedge^k M)s_1(\wedge^k M').$$

We obtain the claim by combining this with the well-known fact [Bh, page 18] that $s_1(\wedge^k A) = \prod_{j=1}^{k} s_j(A)$ for any matrix $A \in GL_n(\mathbb{C})$. □

We will also need the following two elementary facts.

Lemma 5.2. *Let U be a unitary matrix of size d with eigenvalues $\lambda_1, \dots, \lambda_d$. Then the singular values of $(U + U^{-1})/2$ are $|\mathrm{Re}(\lambda_1)|, \dots, |\mathrm{Re}(\lambda_d)|$.*

Lemma 5.3. (i) $\sin(t) \geq t/2$ *if* $0 \leq t \leq \pi/2$.
(ii) $\cos(t) \leq \exp(-t^2/4) \leq \exp(-2t^2/\pi^2)$ *if* $0 \leq t \leq \pi$.

Proof. (i) Consider $f(t) := \sin(t) - t/2$. As $f'(t) = \cos(t) - 1/2$, for $t \in [0, \pi/2]$, we have that

$$f(t) \geq \min\{f(0), f(\pi/2)\} = 0.$$

(ii) Now, again on $[0, \pi/2]$ for $g(t) := \exp(-t^2/4) - \cos(t)$ we have that $g(0) = 0$ and

$$g'(t) = \sin(t) - \frac{t}{2}\exp(-t^2/4) \geq f(t) \geq 0,$$

and so $g(t) \geq 0$. The statement is obvious if $t \in [\pi/2, \pi]$. □

6. Proof of main Theorems

We first prove the following auxiliary statement.

Theorem 6.1. *There is an integer $p_0 > 1$ such that the following statement holds whenever $p \geq p_0$. Let $m \geq 43$ be an integer, $p \geq m$ a prime number, and let $n, s \geq 2$ be integers. Let V be a sequence $A_1, \dots, A_n$ of elements of $S = PSL_m(p)$ of order at least s. Then*

$$\rho_V \leq \frac{2}{p} + \frac{120}{s} + \frac{19}{n^{1/2}}.$$

All theorems from Section 1 will follow from this theorem via some short arguments.

6.1. **Proof of Theorem 6.1.** We start with the identity (4.1)

$$\mathbf{P}(\prod_{i=1}^{n} \hat{A}_i = B) = \frac{1}{|S|} \sum_{\Phi \in \mathrm{Irr}(S)} (\dim \Phi)\, \mathrm{trace}\left(\prod_{i=1}^{n} \frac{\Phi(A_i) + \Phi(A_i^{-1})}{2} \Phi(B^{-1})\right). \tag{6.1}$$

In what follows, we may (and will) assume that $\Phi(X)$ is unitary for any element $X \in PSL_m(p)$. As the absolute value of the trace of any unitary matrix does not exceed its size, we have

$$|\,\mathrm{trace} \prod_{i=1}^{n} \Phi(A_i^{\pm 1})\Phi(B^{-1})| = |\,\mathrm{trace}\, \Phi(\prod_{i=1}^{n} A_i^{\pm 1} B^{-1})| \leq \dim \Phi.$$

Using Proposition 3.3(i), we can easily bound the contribution in the RHS of (6.1) coming from representations of dimension less than

$$d_0 := p^{(m^2-m-1)/2},$$

as the absolute value of this contribution is at most

$$\frac{1}{|S|} \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) < d_0} \chi(1)^2 < \frac{5}{3p}. \tag{6.2}$$

By Proposition 3.3(iii), $k_i := \mathbf{o}(A_i) < p^{m+1} < d_0$. Recall that $s \leq \min\{k_i \mid 1 \leq i \leq n\}$, the minimum order of the elements A_i.

Now we focus on representations Φ of dimension $d \geq d_0$. Choosing p_0 large enough, we may apply Proposition 3.3(iv) to conclude that the eigenvalues of $\Phi(A_i)$ are among the k_i-th roots of unity, with multiplicity at most

$$m_i := \lfloor \frac{3d}{k_i} \rfloor \leq \frac{3d}{k_i}. \tag{6.3}$$

As $\Phi(A_i)$ is unitary, by Lemma 5.2, any singular value of

$$B_i = \frac{1}{2}\left(\Phi(A_i) + \Phi(A_i^{-1})\right)$$

is either 1 or $|\cos(2\pi j/k_i)|$ for some $1 \leq j \leq k_i - 1$. Replacing j by $k_i - j$ if necessary we may assume that $1 \leq j \leq k_i/2$. Furthermore, if $k_i/4 < k_i \leq k_i/2$, we can replace $|\cos(2\pi j/k_i)|$ by $|\cos(\pi(k_i - 2j)/k_i)|$ to get an angle in the range $[0, \pi/2]$. This procedure ensures by Lemma 5.3 that any singular value of B_i is either 1 or

$$\cos(\pi j/k_i) \leq \exp(-2j^2/k_i^2) \tag{6.4}$$

with $1 \leq j \leq k_i/2$, and each such occurs as a singular value of B_i at most $4m_i$ times.

Next we set

$$l_0 := \left\lceil \frac{120d}{s} \right\rceil \geq \frac{120d}{k_i} \geq 40m_i, \tag{6.5}$$

where the inequalities follow from the condition on s and (6.3).

Consider the matrix

$$M = M(\Phi) = \prod_{i=1}^{n} \frac{\Phi(A_i) + \Phi(A_i^{-1})}{2}\Phi(B^{-1}) = (\prod_{i=1}^{n} B_i)\Phi(B^{-1}).$$

Applying Lemma 5.1 repeatedly and using the fact that $s_1(\Phi(B^{-1})) = 1$, we have, for any l, that

$$\prod_{j=1}^{l} s_j(M) \leq \prod_{i=1}^{n}\prod_{j=1}^{l} s_j(B_i). \tag{6.6}$$

Assume that $l > l_0$. As $l_0 \geq 40m_i$, we can write $l = 4m_i a_i + b_i$ with integers $4m_i \leq b_i < 8m_i$ and $4 \leq a_i$. In fact,

$$a_i = \left\lfloor \frac{l - 4m_i}{4m_i} \right\rfloor > \frac{l - 8m_i}{4m_i} > \frac{l}{5m_i}.$$

We are going to show that $\sigma_i := \prod_{j=1}^{l} s_j(B_i)$ is small, for all $1 \leq i \leq n$. As shown above, the multiplicity of any singular value of B_i is at most $4m_i < l/5$. Furthermore, the different singular values of B_i (in decreasing order) are bounded by $\exp(-2j^2/k_i^2)$ with $0 \leq j \leq k_i/2$ by (6.4). We can now bound σ_i from the above by bounding the first b_i singular values of B_i by 1 (note that we chose $b_i \geq 4m_i$), the next $4m_i$ by $\exp(-2/k_i^2)$, the next $4m_i$ by $\exp(-2 \cdot 2^2/k_i^2)$, and so on. It follows that $\sigma_i \leq \exp(-E_i)$, where

$$E_i = 4m_i \cdot \left(\frac{2}{k_i^2} + \frac{2 \cdot 2^2}{k_i^2} + \ldots + \frac{2 \cdot a_i^2}{k_i^2}\right).$$

Since $\sum_{k=1}^{a_i} k^2 > a_i^3/3$ and $a_i > l/5m_i$, we obtain

$$E_i > \frac{8m_i a_i^3}{3k_i^2} > \frac{8l^3}{375k_i^2 m_i^2} \geq \frac{8l^3}{3375d^2} > \frac{l^3}{422d^2},$$

as $k_i m_i \le 3d$ by (6.3). It follows that

$$\sigma_i \le \exp(-l^3/422d^2).$$

Combining this estimate with (6.6), we obtain

$$s_l(M)^l \le \prod_{j=1}^{l} s_j(M) \le \prod_{i=1}^{n} \sigma_i \le (\exp(-l^3/422d^2))^n = \exp(-nl^3/422d^2),$$

whence

$$s_l(M) \le \exp(-nl^2/422d^2)$$

for any $l > l_0$.

Now we have

$$\sum_{l=l_0+1}^{d} s_l(M) \le \sum_{l=l_0+1}^{d} \exp\left(-\frac{nl^2}{422d^2}\right),$$

where the RHS is bounded from above by

$$\int_0^\infty e^{-\frac{nt^2}{422d^2}} dt < \sqrt{\frac{422}{n}} d \int_0^\infty e^{-t^2} dt < \frac{18.3d}{n^{1/2}}.$$

Using the trivial estimate $s_j(M) \le 1$ for $1 \le j \le l_0$ and Lemma 5.1, we conclude that

$$|\operatorname{trace} M| \le l_0 + \sum_{l=l_0+1}^{d} s_l(M) < \lceil \frac{120d}{s} \rceil + \frac{18.3d}{n^{1/2}} \le \frac{120d}{s} + 1 + \frac{18.3d}{n^{1/2}}.$$

Thus, the contribution

$$w(\Phi) = (\dim \Phi) \operatorname{trace}\left(\prod_{i=1}^{n} \frac{\Phi(A_i) + \Phi(A_i^{-1})}{2} \Phi(B^{-1})\right)$$

is at most

$$d^2 \cdot \left(\frac{120}{s} + \frac{1}{d_0} + \frac{18.3}{n^{1/2}}\right)$$

in absolute value, when $d = \dim \Phi$ is at least $d_0 = p^{(m^2-m-1)/2} > 2p$.

Using the identity $\sum_{\Phi \in \mathrm{Irr}(S)} (\dim \Phi)^2 = |S|$ and (6.2), we conclude that the RHS in (6.1) is at most

$$\frac{5}{3p} + \frac{120}{s} + \frac{18.3}{n^{1/2}} + \frac{1}{d_0} < \frac{2}{p} + \frac{120}{s} + \frac{19}{n^{1/2}}$$

proving the theorem.

6.2. **Proof of Theorem 1.4.** Replacing A_i by $A_i^* := \operatorname{diag}(A_i, \det(A_i)^{-1}, I_r)$ and $B^* := \operatorname{diag}(B, \det(B)^{-1}, I_r)$ for a suitable $r \ge 1$, where I_r denotes the identity $r \times r$-matrix, we can assume that $A_i^*, B^* \in SL_{m+r+1}(p)$ with $m + r + 1 \ge 43$. Let $\bar{A}_i$ and $\bar{B}$ denote the image of A_i^*, respectively of B^*, in $PSL_{m+r+1}(p)$. Note that the condition $r \ge 1$ implies that $\mathbf{o}(A_i) = \mathbf{o}(\bar{A}_i)$ for all i. Also, if

$$A_1^{i_1} A_2^{i_2} \dots A_n^{i_n} = B$$

for some $i_j = \pm 1$, $1 \le j \le n$, then

$$\bar{A}_1^{i_1} \bar{A}_2^{i_2} \dots \bar{A}_n^{i_n} = \bar{B}.$$

Hence, when p is sufficiently large, Theorem 6.1 applied to $PSL_{m+r+1}(p)$ implies the bound

$$\frac{2}{p}+\frac{120}{s}+\frac{19}{n^{1/2}}\le 141\cdot\max\left\{\frac{1}{s},\frac{1}{n^{1/2}}\right\},$$

given that $p\ge\min\{s,\sqrt{n}\}$.

6.3. **Proof of Theorem 1.3.** For any $B\in GL_m(\mathbb{C})$ and the sequence $A_1,\dots,A_n$ of elements in $GL_m(\mathbb{C})$, we use Corollary 2.2 to embed $A_1,\dots,A_n,B$ into $GL_m(p)$, for a large prime $p\ge m$. Theorem 1.3 now follows from Theorem 1.4.

6.4. **Proof of Theorem 1.5.** If all $A_1,\dots,A_n$ have order at least s, then we can apply Theorem 1.3. To handle the case when not every A_i has order at least s, let us revisit the setting of Theorem 6.1. Consider

$$\mathbf{P}(\prod_{i=1}^{n}\hat{A}_i=B)=\sum_{\Phi\in\mathrm{Irr}(G)}(\dim\Phi)\,\mathrm{trace}\left(\prod_{i=1}^{n}\frac{\Phi(A_i)+\Phi(A_i^{-1})}{2}\Phi(B^{-1})\right).$$

We have

$$|\,\mathrm{trace}\prod_{i=1}^{n}\frac{\Phi(A_i)+\Phi(A_i^{-1})}{2}\Phi(B^{-1})|\le\sum_{i=1}^{\dim\Phi}s_i(M)$$

where M is the product of $B_i:=(1/2)(\Phi(A_i)+\Phi(A_i^{-1}))$, $1\le i\le n$. Since $s_1(B_i)\le 1$, by Lemma 5.1 we have

$$\sum_{i=1}^{\dim\Phi}s_i(M)\le\sum_{i=1}^{\dim\Phi}s_i(M')$$

where M' is the product of all B_i where A_i has order at least s. Now we can repeat the rest of the proof.

References

[Ap] T. M. Apostol, '*Introduction to Analytic Number Theory*', Undergraduate Texts in Mathematics, New York-Heidelberg, Springer-Verlag, 1976.

[Bh] R. Bhatia, '*Matrix Analysis*', Springer 1996.

[E] P. Erdős, On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc.* **51** (1945), 898–902.

[EM] P. Erdős and L. Moser, Elementary problems and solutions, *Amer. Math. Monthly,* **54** (1947), no. 4, 229–230.

[Es] C. G. Esséen, On the Kolmogorov-Rogozin inequality for the concentration function, *Z. Wahrsch. Verw. Gebiete* **5** (1966), 210–216.

[FF] P. Frankl and Z. Füredi, Solution of the Littlewood-Offord problem in high dimensions, *Ann. of Math.* **128** (1988), 259–270.

[FK] H. Furstenberg and H. Kesten, Products of random matrices, *Ann. Math. Statist.* 31 (1960), no. 2, 457–469.

[FG] J. Fulman and R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.

[G] D. Gluck, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229–266.

[Gr] J. Griggs, The Littlewood-Offord problem: tightest packing and an M-part Sperner theorem, *Europ. J. Combin.* **1** (1980), 225–234.

[H] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, *Period. Math. Hungar.* **8** (1977), no. 3-4, 197–211.

[Kle1] D. Kleitman, On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors, *Adv. Math.* **5** (1970) 155–157.

[Kle2] D. Kleitman, Some new results on the Littlewood-Offord problem, *J. Combin.Theory Ser. A* **20** (1976), no. 1, 89–113.

[Kle3] D. Kleitman, On a lemma of Littlewood and Offord on the distribution of certain sums, *Math. Z.* **90** (1965), 251–259.

[Kol1] A. Kolmogorov, Two uniform limit theorems for sums of independent random variables, *Theor. Probab. Appl.* **1** (1956), 384–394.

[Kol2] A. Kolmogorov, Sur les propriétés des fonctions de concentrations de M. P. Lévy, *Ann. Inst. H. Poincaré* **16** (1958), 27–34.

[LMT] M. Larsen, G. Malle, and Pham Huu Tiep, The largest irreducible representations of simple groups, *Proc. Lond. Math. Soc.* **106** (2013), 65–96.

[LST] M. Larsen, A. Shalev, and Pham Huu Tiep, The Waring problem for finite simple groups, *Ann. of Math.* **174** (2011), 1885–1950.

[LO] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III, *Rec. Math. Mat. Sbornik* N.S. **12** (1943), 277–286.

[LV] E. Lindenstrauss and P. P. Varju, Random walks in the group of Euclidean isometries and self-similar measures, *preprint; arXiv:1405.4426.*

[Ng] Hoi H. Nguyen, Inverse Littlewood-Offord problems and the singularity of random symmetric matrices, *Duke Math. J.* **161** (2012), 545–586.

[Ngv] Hoi H. Nguyen and Van H. Vu, Optimal Littlewood-Offord theorems, *Adv. Math.* **226** (2011), 5298–5319.

[NV] Hoi H. Nguyen and Van H. Vu, Small ball probability, inverse theorems, and applications, in: '*Erdős Centennial*', pp. 409–463, Bolyai Soc. Math. Stud. **25**, János Bolyai Math. Soc., Budapest, 2013.

[Rog] B. A. Rogozin, An estimate for concentration functions, *Theor. Probab. App* **1** (1961), 94–97.

[RV] M. Rudelson and R. Vershynin, The Littlewood-Offord problem and invertibility of random matrices, *Adv. Math.* **218** (2008), 600–633.

[SC] L. Saloff-Coste, Random walks on finite groups, in: '*Probability on Discrete Structures*', 263–346, Encyclopaedia Math. Sci., **110**, Springer, Berlin, 2004.

[SSz] A. Sárközy and E. Szemerédi, Über ein Problem von Erdős und Moser, *Acta Arithmetica* **11** (1965), 205–208.

[St] R. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Algebraic Discrete Methods* **1** (1980), no. 2, 168–184.

[TV1] T. Tao and Van H. Vu, From the Littlewood-Offord problem to the circular law: universality of the spectral distribution of random matrices, *Bull. Amer. Math. Soc.* (N.S.) **46** (2009), no. 3, 377–396.

[TV2] T. Tao and Van H. Vu, A sharp inverse Littlewood-Offord theorem, *Random Structures Algorithms* **37** (2010), no. 4, 525–539.

[TV3] T. Tao and Van H. Vu, The Littlewood-Offord problem in high dimensions and a conjecture of Frankl and Füredi, *Combinatorica* **32** (2012), no. 3, 363–372.

[VWW] Van H. Vu, M. M. Wood, and P. M. Wood, Mapping incidences, *J. Lond. Math. Soc.* **84** (2011), 433–445.

Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA
E-mail address: tiep@math.arizona.edu

Department of Mathematics, Yale University, New Haven , CT 06520, USA
E-mail address: van.vu@yale.edu